Title: **Responsible Use of Information Technology Resources**

Initial Action:	5/29/96
Board Resolution:	96-128
Last Revised:	
Policy:	5/29/96
Procedure:	8/29/2023
Last Reviewed:	6/1/04
Effective:	8/29/2023
Next Review:	August 29, 2026
Responsibility:	Computer Services

Policy:

It is the policy of Cecil College (hereafter "College") that all persons who are permitted to use the College's information technology resources (including computing systems, software, internal and external data networks, information and communication systems) comply with all applicable laws, contractual agreements, licenses, and copyright provisions, and observe the highest standard of ethics in their use of those resources. The College offers users of its information technology resources no assurance of privacy or confidentiality, and reserves the right to access, monitor and inspect all information technology systems to ensure that all College information technology resources are used in a lawful manner and in compliance with this policy.

Procedure:

I. Introduction

Cecil College provides information technology resources to facilitate the educational process and to further the administrative efforts in support of research and instruction for faculty, staff and students of Cecil College. Information technology resources include computing systems, hardware and software, as well as internal and external data networks. For purposes of this policy, a "user" is any individual who uses, logs in, attempts to use, or attempts to log into a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software, or both. The use of said resources must be consistent with the mission statement of the College and with facilitating the exchange of knowledge and information, while encouraging resource sharing and collaborative projects in education and research.

The Responsible Use of Information Technology Policy for Cecil College contains the governing philosophy for regulating faculty, staff, student, and other permitted users of the College's information technology resources. It spells out the general principles regarding the appropriate use of information technology equipment, hardware, software, and networks. All users of College information technology resources are also bound by local, state, and federal laws relating to copyright, information security, and electronic media. All Cecil College faculty and staff are responsible for acting in accordance with this policy, and through their leadership and example, ensuring full compliance of this policy throughout the College community. The Division of Information Technology, the Vice President of Student Services and Enrollment Management ("Student Services") and the Executive Director of Human Resources (HR) are tasked with disseminating this policy to all users and enforcing all policy provisions.

Access to the College's information technology resources is a privilege granted to the College's faculty, staff, and students, which may be enhanced, limited, restricted or withdrawn by the College at any time. Individuals other than College faculty, staff, and students may be permitted access to College information technology resources, provided such access does not interfere with the computing and/or network resource needs of the College community, and that the users comply with all College policies (including this policy), and all applicable licenses, contractual agreements, federal, state, and local laws. Access by such permitted users is solely within the discretion of the College, and may be granted, limited, restricted or withdrawn by the College at any time.

College information technology resources are provided for the educational, research, administrative and employment-related purposes of the College community. College information technology resources may not be used for the transmission or storage of commercial or personal advertisements or solicitations, phishing/SPAM, destructive programs (viruses and/or self-replicating codes), abusive, harassing, slanderous, libelous, obscene, offensive, profane, pornographic, threatening, or sexually explicit material, or for any other unauthorized use. This policy applies equally to all College-owned or College-leased equipment. Limited personal use of the College's information technology resources is permitted, provided that such use does not interfere with or disrupt College business and complies with all other requirements of this policy.

Users of College information technology resources must guard against abuses that disrupt or threaten the viability of any system, including those at the College and those on networks accessed by the College's external network communications. Access to information technology resources without proper authorization from the data owner or without College approval, unauthorized use of College facilities, and intentional corruption or misuse of all technology information resources are direct violations of the College's standards for conduct.

To ensure that College information technology resources are used in compliance with this policy, and in a lawful manner, Cecil College reserves the right, but not the duty, to inspect and review all systems and their use, without notice, including the right to enter the email system at any time to review, copy or delete any stored messages or information. *Faculty, staff, students, or other permitted users should not have any expectation of privacy in anything they create, send, or receive using the College* *information technology resources.* As a condition of using the College’s information technology resources, including email, faculty, staff, students and other permitted users consent to allow the College’s Information Technology staff to inspect, review and copy email messages and other electronic communications, contained in storage, with the permission of the Chief Information Officer ~~or Vice President of Student Services~~.

II. Terms and Conditions for Use of Cecil College Information Technology Resources

1. Information technology users shall not interfere with or disrupt information technology systems or resources. Disruption includes, but is not limited to, distribution of unsolicited advertising, creation and/or propagation of computer worms or viruses, transmission of slanderous and/or harassing materials, distribution or storage of chain letters, and using College facilities to gain unauthorized entry to any other system, whether internal or external to the College network.

2. Users must respect the usage privileges of others, both on the College campus and at all sites accessible by the College's external network communications. It is prohibited to divulge the College’s password of any member of the College community.

3. Users shall not intentionally copy or modify files, electronic mail or other data, or passwords belonging to other users (whether maintained on College information technology systems or on networks accessed by the College's external network communications) or develop or retain programs for that purpose, without the authorization of the Chief Information Officer.

4. Users shall not attempt to install, alter, or damage either the hardware or the software components of a College computing system or network, without proper authorization from the Chief Information Officer.

6. Users shall not use any College information technology resources for any purpose prohibited by law.

7. Users shall report any incident of harassment, and the receipt, viewing, display or copying of any inappropriate or offensive email, to the Chief Information Officer or the Vice President of Student Services. All such reports or complaints will be thoroughly investigated.

8. All software found on College systems is licensed by the College and as such may not be copied for personal use, transferred to non-College equipment or modified in anyway. Users will comply with all licenses and copyright laws with respect to computer software.

9. Unauthorized users shall not access any College administrative information systems that are confidential, without prior permission. This prohibition exists even if the software system does not automatically preclude access to this information.

10. College does not guarantee the accuracy and quality of the information obtained through use of College information technology resources. No warranties for information technology resources are expressed or implied. College will not be responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties.

11. Student email and user accounts will be deleted two academic years after the last semester in which a student is registered for classes. When an employee ceases employment with the College for any reason, access to their email and user accounts will be terminated, on the last date of employment. Former employee email accounts will be deleted after two years.

III. Implementation

Cecil College's Chief Information Officer and IT staff are responsible for the implementation of this policy. Faculty, staff, students, and any other permitted users of the College's information technology resources are responsible for following all the requirements contained in this policy.

IV. Enforcement

Alleged violators of this policy shall be subject to the procedures outlined in the applicable Cecil College policy, the College Catalog (Student Code of Conduct), and the Student Handbook. Cecil College treats violations of its information technology policy seriously and reserves the right to pursue criminal and civil prosecution of violators.

V. Guidelines for Creation and Maintenance of cecil.edu pages

1. All "cecil.edu" pages created for departments or organizations within Cecil College and placed on the College web server are considered official representations of the college and thus must be in compliance with the stated mission and standards for the College, as found in the Cecil College Faculty Handbook, College Catalog (Student Misconduct Policy), and Student Handbook.

2. All pages for students/student organizations must be approved by the organization's faculty or staff advisor and the Vice President of Student Services or designee prior to publications on cecil.edu.

3. All departmental pages must be approved by the appropriate Vice President or designee.

4. Cecil College reserves the right to revise or remove pages from the College web servers at any time.

VI. Disciplinary and Appeal Procedures

Disciplinary Procedures for Students:

1. Students who are charged with a violation of this policy will be referred to the Director of Student Life of Student Services or designee for possible disciplinary action.

2. Students who are found to have violated this policy may have their information technology resource privileges suspended or revoked, and/or be subjected to other disciplinary or legal action, depending on the seriousness or frequency of the violation. Additionally, the Vice President or designee may refer the student for appropriate counseling in the proper use of information technology resources. Serious violations could result in dismissal from the College and/or criminal prosecution.

3. Based on the principles of standard classroom management, faculty reserve the right to dismiss any student (temporarily pending a disciplinary hearing) from a class if the student's use of information technology resources in that class is not consistent with the academic objectives of the course.

4. Students appeals of any finding of an information technology violation will be adjudicated as detailed in the Student Code of Conduct. This process is described in detail in the College Catalog.

Disciplinary Procedures for Faculty/Staff:

1. Faculty or Staff who are charged with violation of this computer policy will be also referred to the appropriate Vice President, Dean, or Administrator who will contact Human Resources for possible disciplinary action.

2. Faculty or Staff who have violated this policy may have their information technology resource privileges suspended or revoked, and/or be subjected to other disciplinary or legal action, depending on the seriousness or frequency of the violation. Additionally, the College may refer the faculty or staff member for appropriate counseling in the proper use of information technology resources. Serious violations could result in discharge from employment and/or criminal prosecution.

3. Faculty and Staff may appeal any finding of an information technology violation through the applicable College grievance procedures, if any such procedure applies to the employee, as detailed in the College Faculty Handbook or applicable College policy. If no grievance procedure applies, any determination below the level of President may be appealed to the President, but a decision by the President will be considered final.

Acknowledgement of Responsible Use of Information Technology

You are about to access a Cecil College computer/device and or computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the computer or network for any purpose including criminal prosecution.

Use of the Cecil College computer systems is contingent upon compliance with the College's **Responsible Use of Information Technology Resources** policy and the following rules:

1. A user may not attempt to access or modify any data or programs unless you have been granted permission.
2. A user may not make unauthorized copies of any copyrighted software for personal use.
3. A user may not engage in any activity which harasses other users, makes personal profit or constitutes personal business, is defined as gambling activity, endangers lives or livelihoods, accesses or distributes pornographic material, or engages in criminal activity.
4. A user may not download, install, or run any program from the internet without the approval of your instructor or a network administrator.
5. A user may not install or run any software which is not supplied or authorized by the College.
6. A user may not run password tracking, password cracking, or virus generating programs for any reason.
7. A user may not generate an inordinate amount of traffic that adversely affects others.
8. A user is prohibited from sharing or loaning an account to any individual not assigned to it. All user accounts, including logon, email access, and network storage are for use by the individual or individuals to which it is assigned.
9. A user is strictly prohibited from stealing, rearranging, or damaging any College computer/device or network equipment, facilities or property and will be reported to the police. This includes all public computer labs, network hubs, wiring and links.
10. A user must log-out of public devices and all accounts when finished to ensure they are not held responsible for policy violations occurring on their account.
11. A user (students, faculty, and staff) is assigned an email for the purpose of adhering to the College's mission and should not be used for fraudulent, harassing, or obscene purposes.
12. Automatic forwarding of your cecil.edu email account to such personal and/or third-party email services is not permitted.

Unauthorized or illegal use of a Cecil College electronic device will not be tolerated and may result in disciplinary action, criminal prosecution, or both.